JC02 Rec'd PCT/PTO 28 MAR 2002

FORM PTO-1390 (Modified) (REV 11-2000) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER	U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR)
RCA 89826	10/089506

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/US00/26060	22 SEPTEMBER 2000 (22.09.00)	28 SEPTEMBER 1999 (28.09.99)

TITLE OF INVENTION

SYSTEM AND METHOD FOR INITIALIZING A SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP) AGENT

APPLICANT(S) FOR DO/EO/US

William Henry Yost

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include items (5), (6), (9) and (24) indicated below.
4. ☐ The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. ☒ A copy of the International Application as filed (35 U.S.C. 371 (c) (2))
   a. ☐ is attached hereto (required only if not communicated by the International Bureau).
   b. ☒ has been communicated by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☐ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
   a. ☐ is attached hereto.
   b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371 (c)(3))
   a. ☐ are attached hereto (required only if not communicated by the International Bureau).
   b. ☐ have been communicated by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☐ An oath or declaration of the inventor(s) (35 U.S.C. 371 (c)(4)).
10. ☐ An English language translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371 (c)(5)).
11. ☒ A copy of the International Preliminary Examination Report (PCT/IPEA/409).
12. ☒ A copy of the International Search Report (PCT/ISA/210).

Items 13 to 20 below concern document(s) or information included:

13. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
14. ☒ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
15. ☒ A **FIRST** preliminary amendment.
16. ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
17. ☐ A substitute specification.
18. ☒ A change of power of attorney and/or address letter.
19. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825.
20. ☐ A second copy of the published international application under 35 U.S.C. 154(d)(4).
21. ☐ A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
22. ☒ Certificate of Mailing by Express Mail
23. ☒ Other items or information:

Return Postcard Receipt

EXPRESS MAIL NO: EL 722193678 US **DATE OF DEPOSIT: MARCH 28, 2002**

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR)	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
10/089506	PCT/US00/26060	RCA 89826

24. The following fees are submitted:.

BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)) :

		CALCULATIONS PTO USE ONLY
☐	Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO **$1040.00**	
☒	International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO **$890.00**	
☐	International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO **$740.00**	
☐	International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4) **$710.00**	
☐	International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)-(4) **$100.00**	
	ENTER APPROPRIATE BASIC FEE AMOUNT =	**$890.00**
	Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (e)).	**$0.00**

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	5 - 20 =	0	x $18.00	**$0.00**	
Independent claims	1 - 3 =	0	x $84.00	**$0.00**	
Multiple Dependent Claims **(check if applicable)**.			☐	**$0.00**	
	TOTAL OF ABOVE CALCULATIONS =			**$890.00**	
☐	Applicant claims small entity status. See 37 CFR 1.27). The fees indicated above are reduced by 1/2.			**$0.00**	
	SUBTOTAL =			**$890.00**	
	Processing fee of **$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (f)). +			**$0.00**	
	TOTAL NATIONAL FEE =			**$890.00**	
☒	Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31) **(check if applicable).**			**$40.00**	
	TOTAL FEES ENCLOSED =			**$930.00**	
				Amount to be: refunded	$
				charged	$

a. ☐ A check in the amount of _____ to cover the above fees is enclosed.

b. ☒ Please charge my Deposit Account No. **07-0832** in the amount of **$930.00** to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. **07-0832** A duplicate copy of this sheet is enclosed.

d. ☐ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. **Credit card information should not be included on this form.** Provide credit card information and authorization on PTO-2038.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Mr. Joseph S. Tripoli
THOMSON multimedia Licensing Inc.
Patent Department
P. O. Box 5312
Princeton, New Jerey 08540

SIGNATURE

JOSEPH J. LAKS
NAME

27,914
REGISTRATION NUMBER

MARCH 28, 2002
DATE

EXPRESS MAIL LABEL NO. EL 722193678 US RCA 89626

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : William Henry Yost

Filed : September 22, 2000 - PCT National Phase of PCT/US00/26060

For : SYSTEM AND METHOD FOR INITIALIZING A SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP) AGENT

PRELIMINARY AMENDMENT

Hon. Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Sir:

In the US national phase application of PCT/US00/26060 please enter the following amendments.

IN THE SPECIFICATION:

Please amend the specification as follows:

Page 1, After the title, insert the following:

--This application claims the benefit under 35 U.S.C. § 365 of International Application No. PCT/US00/26060, filed September 22, 2000, which claims the benefit of U.S. Provisional Application 60/156,385, filed September 28, 1999.—

IN THE ABSTRACT:

Page 19 Please add the Abstract supplied on a separate sheet herewith.

EXPRESS MAIL LABEL NO. EL 722193678 US RCA 89626

REMARKS

The specification has been amended to include a reference to the priority applications.

An Abstract is supplied on a separate sheet.

No fee is believed to have been incurred by virtue of this amendment. However, if a fee is incurred on the basis of this amendment, please charge such fee against deposit account 07-0832.

Respectfully submitted,
William Henry Yost

By: Joseph J. Laks
Attorney for Applicant
Registration No. 27,914
609/734-9813

THOMSON multimedia Licensing Inc.
Patent Operation
PO Box 5312
Princeton, NJ 08543-5312

Date: March 28, 2002

ABSTRACT OF THE DISCLOSURE

A system and method for initializing a SNMP agent in SNMPv3 mode. In one aspect of the invention, a method is provided that allows an operator to securely enter the initial SNMPv3 privacy and authentication keys into a SNMPv3 device and cause the device to enter in SNMPv3 mode. The SNMP manager and SNMP agent both generate an associated random number and public value. The SNMP manager passes its public value to the SNMP agent in a configuration file, which causes a proprietary MIB element in the SNMPv3 device to be set with the public value of the SNMP manager. The SNMP manager reads the public value of the SNMP agent through a SNMP request using an initial valid user having access to the public value of the SNMP agent. The SNMP agent and SNMP manager each independently compute a shared secret using the Diffie-Hellman key exchange protocol. The SNMP manager and SNMP agent each independently convert the shared secret into the same readable password, convert the readable password into the same secret key and set the initial authentication key and the initial privacy key to the value of the secret key.

SYSTEM AND METHOD FOR INITIALIZING A SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP) AGENT

BACKGROUND

1. Technical Field:

The present application relates generally to a system and method for initializing an SNMP (simple network management protocol) agent and, in particular, a system and method for generating authentication and privacy keys for a first user of a SNMPv3 network-managed device and securely entering the keys into the device to initialize the device into SNMPv3 mode.

2. Description of Related Art:

In general, the SNMP is a standard application-layer protocol that is employed in a network to facilitate the exchange of management information between networked devices. The SNMPv3 framework defines standard security and access control protocols known, respectively, as the User-Based Security Model (USM) and View-Based Access Control Model (VACM). The SMMPv3 standard is an extensible "bare-bones" protocol that allows vendors to incorporate proprietary MIB (management information base) elements and applications to execute on top of the standard SNMP framework.

An SNMP network generally comprises a plurality of distributed SNMP entities each comprising one or more SNMP agents and one or more SNMP managers (although an entity may comprise both an agent and manager) that communicate using SNMP messages. An SNMP manager (or NMS (network management station)) is responsible for managing one or more SNMP agents within the domain of the SNMP manager. An SNMP agent is included on each node (or host) of the network (e.g., computer, server, etc) that is managed by an SNMP manager. Each agent is responsible for collecting and maintaining information about its environment and providing such information to a respective SNMP manager and responding to manager commands to alter the local configuration or operating parameters of the managed node. Each SNMP agent maintains a local MIB (management information base, which is a virtual information store that comprises management information, i.e., current and historical information about the local configuration and traffic of the managed device (node). More specifically, the SNMP agent MIB comprises a collection of managed objects within the device to be managed, wherein collections of related objects are defined in MIB modules.

In an SNMPv3 mode, an SNMP agent implements the standard USM (user-based security model), wherein the configuration parameters for the USM are managed via MIB elements defined by the SNMP-USER-BASED-SM-MIB module (which is described in detail, for example, in RFC 2574, "User-Based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", by Blumenthal et al, April 1999). As is known in the art, for USM, all valid users associated with an SNMPv3 agent utilize a unique secret authentication key and unique privacy key (and standard protocols) for authentication incoming/outgoing messages and encrypting/decrypting the payload of outgoing/incoming messages. Furthermore, in an SNMPv3 mode, the SNMP agent utilizes the View-based Access Control Model (VACM) is utilized by the agent (in response to a call by an SNMP application) to determine whether a specific type of access (read, write) is authorized for a SNMP manager requesting to retrieve or modify local MIB managed data, or whether the manager is authorized to receive notifications (traps) from the agent. The configuration parameters for the VACM are managed via MIB elements defined by the SNMP-VIEW-BASED-ACM-MIB as described in detail, for example, in RFC 2575, "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP) ", by Wijnen, et al, April, 1999).

Various applications and network architectures implement the SNMP framework. For instance, the SNMP protocol has been selected as the communications protocol for management of DOCSIS (Data Over Cable Service Interface Specifications)-based cable modem systems. The DOCSIS cable modems are configured with SNMP agents, which allows a manager (operator of the DOCSIS cable modem system) to remotely manage and configure the cable modems of the end users. The current DOCSIS cable modem system framework, however, does not provide a standard protocol for entering the initial authentication and privacy keys into a cable modem to initialize the cable modem in SNMP v3 mode and vendors must provide proprietary protocols for performing this initialization.

The SNMPv3 framework recommends that the ***usmUserTable*** be populated out of band, e.g., not using SNMP (i.e., the first user must be created and its authorization and privacy keys entered in the managed device without using SNMP). SNMP can not be used for this initialization because it provides privacy only by using the privacy key of an already existing user. If the number of agents to be initialized is small, an initialization process can be performed via a console port and manually. If the number of agents is large, such as in cable

modem systems, the manual approach is burdensome and does not scale well. Accordingly, a system and method that would provide a secure method for entering the privacy and authentication keys into a cable modem in a DOCSIS system to initialize the modem in SNMPv3 mode is highly desirable.

SUMMARY OF THE INVENTION

The present invention is directed to a system and method for initializing a SNMP agent in SNMPv3 mode. In one aspect of the invention, a method is provided that allows an operator to securely enter the initial SNMPv3 privacy and authentication keys into a SNMPv3 device and cause the device to enter in SNMPv3 mode. The SNMP manager and SNMP agent both generate an associated random number and public value. The SNMP manager passes its public value to the SNMP agent in a configuration file, which causes a proprietary MIB element in the SNMPv3 device to be set with the public value of the SNMP manager. The SNMP manager reads the public value of the SNMP agent through a SNMP request using an initial valid user having access to the public value of the SNMP agent. The SNMP agent and SNMP manager each independently compute a shared secret using the Diffie-Hellman key exchange protocol. The SNMP manager and SNMP agent each independently convert the shared secret into the same readable password, convert the readable password into the same secret key, and then set the initial authentication key and the initial privacy key to the value of the secret key.

In another aspect of the present invention, the configuration file passes the CMTS Diffie-Hellman public value to the modem using a proprietary configuration file object type, wherein the proprietary configuration file object has the advantage of not causing SNMP v1/v2c capable only modems to reject the configuration file because they do not understand a standard SNMP MIB object (configuration file element type 11) that may be used to set a proprietary MIB element in the modem.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram of system for initializing a SNMPv3 agent according to an exemplary embodiment of the present invention; and

Fig. 2 is a flow diagram of a method for initializing a SNMPv3 agent according to one aspect of the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

It is to be understood that the present invention may be implemented in various forms of hardware, software, firmware, special purpose processors, or a combination thereof. Preferably, the present invention is implemented in software as an application comprising program instructions that are tangibly embodied on one or more program storage devices (e.g., magnetic floppy disk, RAM, CD ROM, ROM, Flash memory, etc.) and executable by any device, machine or platform comprising suitable architecture. It is to be further understood that because some of the system components and method steps are preferably implemented in software, the actual connections may differ depending upon the manner in which the present invention is programmed.

Referring to Fig. 1, block diagram illustrates a system 10 for initializing a SNMPv3 managed device according to an exemplary embodiment of the present invention. More specifically, the system 10 comprises a DOCSIS cable modem system that provides transparent bi-directional transfer of Internet Protocol (IP) packets (received/transmitted over a backbone network 14, e.g., the Internet) between a CMTS (cable modem termination system) 16 and a SNMPv3 cable modem 18 over an all coaxial or hybrid-fiber/coaxial (HFC) cable network 17. As is known in the art, the CMTS 16 performs functions such as providing an interface between IP traffic and RF (radio frequency) modulation/transmission of the IP packets and assigning IP addresses to cable modem18. It is to be understood that only one cable modem is shown for illustrative purposes, but the system 10 may comprise hundreds of cable modems.

The system 10 comprises a NMS (network management station) 11 located on the backbone network 14 for managing the CMTS 16 and DOCSIS cable modem 18. The NMS 11 comprises a user interface 12 (e.g., a GUI (graphic user interface)) and a SNMP manager 13 of conventional architecture for communicating with the SNMP agents 19 of cable modem 18 via SNMP messages. The system 10 further comprises a remote server facility 15 that is accessible by the cable modem 18 for, e.g., downloading a configuration file comprising parameters that are used for configuring the cable modem 18. For instance, as explained in detail below, the configuration file comprises objects that are used to initialize the SNMP agent 19 in SNMPv3 mode using a proprietary Diffie-Hellman Key exchange protocol for entering the initial authentication and privacy keys into the cable modem 18. In general, this protocol allows an operator at the NMS (manager) 11 to securely enter the initial SNMPv3

privacy and authentication keys into the modem 18 and cause the modem 18 to enter SNMPv3 mode using a Diffie-Hellman key exchange. The manager 13 provides its public value to the modem 18 via the configuration file (located, for example, in server 15). The manager 13 reads the public value of the modem 18 via SNMPv3 using a standard default ***usmUser*** which has access only to these values (and the standard 'system' group). Via the DH exchange, the manager 13 and the cable modem 18 can agree on a common shared secret which is used to populate the key values for another standard ***usmUser*** who has access to the ***usmUserTable*** to create and delete additional users. The manager 13 can then populate that table as necessary.

In accordance with the present invention, the cable modem 18 comprises an MIB that comprises proprietary MIB module and associated MIB elements for effecting a Diffie-Hellman key exchange. More specifically, the MIB 20 comprises a proprietary MIB module referred to herein as **TCE-DCM105-MIB** which defines MIB elements such as ***tceDCM105KickstartMyPublic*** and ***tceDCM105KickstartMgrPublic*** objects that are employed for an SNMPv3 initialization process. These MIB elements provide a mechanism for the SNMPv3 agent 19 (in the cable modem 18) and the SNMP manager 13 to perform a Diffie-Hellman key exchange to place the private keys for the first valid user into the cable modem 18. The ***tceDCM105KickstartMgrPublic*** object is set to the Diffie-Hellman public value of the manager 13 during a registration process. There are various mechanisms by which the public value of the manager 13 is transferred to the agent. Preferably, this transfer is performed via the configuration file (e.g., in remote server 15) that is downloaded by the cable modem 18 during the cable modem registration process. The value of the ***tceDCM105KickstartMyPublic*** MIB element comprises the Diffie-Hellman public value of the agent 19 that the agent 19 publishes for access by the manager 13 via SNMP after the registration process. Preferably, the manager 13 reads the content of ***tceDCM105KickstartMyPublic*** using an initial user having a *securityName*, e.g., "docsisInit", with no authentication. A preferred initialization process will now be described in further detail with reference to the flow diagram of Fig. 2.

The flow diagram of Fig. 2 illustrates a method for initializing a SNMPv3 agent according to one aspect of the present invention. In Fig. 2, steps 100-108 represent steps that are executed by the SNMPv3 agent and steps 200-208 represent steps that are executed by the manager. Upon initialization/power up of the cable modem, proprietary software loaded in the cable modem causes the SNMP agent to create an SNMPv3 user named "docsisInit" of

security level *noAuthnoPriv* and generate the appropriate USM and VACM entries (step 100). This initial valid user (which is used by the manager to access, e.g., the ***tceDCM105KickstartMyPublic*** MIB element of the modem) will only have read access to the *tceDCM105Kickstart group*, the system group, and the generic traps. Next, the agent generates a random number r_1 preferably up to 128 bytes in length (step 101). Then, using the well-known Diffie-Hellman protocol, the agent will convert its random number r_1 to a public value P_1 of the agent (step 102). More specifically, the agent's public value $P1 = g^{r1} \ Mod \ p$, where g is the base from the set of Diffie-Hellman parameters, p is the prime from those parameters, and r_1 is the random integer selected by the agent in the interval $2^{(l-1)} \leq r1 < p - 1$, where l is the length of the private, random value r_1 in bits. The public value P_1 is expressed as an OCTET STRING "PV" of length "k" which satisfies $y(\mathbf{integer public value}) = \sum_{i=1}^{k} 2^{(8(k-i))} PVi$, where $PV_1, ..., PV_k$ are the octets of PV from first to last, and where $PV_1 \neq 0$. In addition, the following Diffie-Hellman parameters (Oakley group #2, RFC 2409, sec. 6.1, 6.2) are preferably used:

$g = 2$;

p = FFFFFFFF FFFFFFFF C90FDAA2 2168C234 C4C6628B 80DC1CD1
29024E08 8A67CC74 020BBEA6 3B139B22 514A0879 8E3404DD
EF9519B3 CD3A431B 302B0A6D F25F1437 4FE1356D 6D51C245
E485B576 625E7EC6 F44C42E9 A637ED6B 0BFF5CBB6 F406B7ED
EE386BFB 5A899FA5 AE9F2411 7C4B1FE6 49286651 ECE65381
FFFFFFFF FFFFFFFF; and

$l = 64$.

The agent publishes its public value P_1 in the MIB element ***tceDCM105KickstartMyPublic*** (step 103).

During a registration process, the SNMP manager will generate its random number r_2, which is preferably up to 128 bytes in length (step 200). The manager then transforms its random number r_2 to a public value P_2 using the Diffie-Hellman key exchange protocol (step 201) in the same manner as the agent and using the same parameter set as described above.

In the DOCSIS framework, during registration, as is known in the art, the cable modem attempts to establish network connectivity by, e.g., transmitting a DHCP (dynamic host configuration protocol) request to the CMTS to obtain an IP address and other parameters

that are needed to establish IP connectivity. The CMTS will transmit a DHCP response comprising, e.g., the name and location, e.g., the IP address of a TFTP (trivial file transfer protocol) server (such as the remote server 15 in Fig. 1), of a configuration file that is accessible by the cable modem. Using the information in the DHCP response, the SNMPv3 cable modem will download the appropriate configuration file via TFTP.

In accordance with the present invention, the manager transfers its public value P_2 to the agent via the configuration file (step 202) (which is downloaded by the modem) in one of several ways. In the exemplary embodiment illustrated in Fig. 2, this is performed using an SNMP "Set" MIB Object in the configuration file (i.e., the DOCSIS standard configuration file element type 11) to set the ***tceDCM105KickstartMgrPublic*** MIB element (in the cable modem) to the public value P_2 of the manager (step 104). Other embodiments for transferring the public value P_2 of the manager to the cable modem are described below.

When the agent determines that the ***tceDCM105KickstartMgrPublic*** has been set to the manager's public value, the agent computes a shared secret ***SK*** from its random number r_1 and the manager's public value P_2 via the Diffie-Hellman key exchange protocol (step 105). More specifically, the SNMPv3 agent computes the shared secret $SK = P2^{r1} \; Mod \; p$, where p is the DH prime from the preferred common parameters described above.

Next, in a preferred embodiment, the SNMPv3 agent converts the shared secret ***SK*** to privacy and authentication keys as follows. First, the agent transforms the shared secret ***SK*** into a readable password of preferably16 characters (or fewer) (step 106). Preferably, this is performed by discarding any OCTETS (in the ***SK*** string) beyond the 16th octet and then performing the following on each remaining octet:

a.. if (octet > 0x7F), then octet = octet B 0x80; // Clear the top bit

b. if (octet ≤ 0x20) octet = octet + 0x40; // Re-Map control codes

c. if(octet = 0x7F) octet = octet - 1; // Re-map delete character.

Advantageously, this process of generating a readable password allows an operator at the NMS to easily enter the password (as opposed to entering the shared secret octet string).

Second, the readable password is then translated into a 16 byte key, ***KC*** (step 107). Preferably, this step is performed using the algorithm described in Appendix A, section A.1, paragraph (2) of RFC 2574 "AUser-based Security Model (USM) for version 3 of the Simple Network Management Protocol". More specifically, a string of length 1,.048, 576 octets is

generated by repeating the value of the password as often as necessary, truncating accordingly, and using the resulting string as the input to the MD5 algorithm (which is well-known in the art) to generate a digest (termed "digest 1"). Then, a second string is formed by concatenating digest 1, the SNMP engine's ***snmpEngineID*** value, and digest 1. This string is used as input to the MD5 algorithm. The resulting digest is the 16 byte key.

The SNMPv3 agent then generates an SNMPv3 user (provisioned user) referred to herein as "docsisProv" and generates appropriate USM and VACM table entries (as discussed in detail below) of security level ***AuthPriv*** with read/write access to the SNMPv3 tables, and then preferably sets both the privacy key and authentication key (of the provisioned user) to the value of the16 byte key, ***KC*** (step 108). The agent will use this same 16 byte key, ***KC*** for any other users created in the SNMPv3 tables by the configuration file. This ends the modem registration process.

Upon completion of registration, the manager can confirm the modem has entered SNMPv3 mode by reading a non-zero length OCTET STRING (i.e., the agent's public value P_1) from the ***tceDCM105KickstartMyPublic*** MIB element (step 203). The manager will read this value using the initial user "docsisInit" (security level ***noAuthNoPriv***) via an SNMP "Get" command. The manager will use its random number r_2 and the agent's public value P_1 (i.e., the ***tceDCM105KickstartMyPublic*** value) to compute the shared secret ***SK*** (via the Diffie-Hellman key exchange algorithm) (step 204). This is the same shared secret ***SK*** computed by the agent. Next, the manager computes the same readable password for the "docsisProv" user from the shared secret ***SK*** (step 205), and then transforms the readable password to the value of ***KC*** (step 206) using the same process as the agent (described above in steps 106-107). The manager will then set the authentication and privacy keys for the provisioned user to the value of ***KC*** (step 207). It is to be appreciated that the Diffie-Hellman key exchange ensures that both the agent and the manager compute the same 16 character password without revealing it. It is to be appreciated that the security of this approach is directly related to the strength of the authorization security of the out of band provisioning of the manager's public value P_2.

The manager may then create other SNMPv3 users by altering the SNMPv3 tables (i.e., accessing the SNMP-USER-BASED-SM-MIB and SNMP-VIEW-BASED-ACM-MIB) using the "docsisProv" user and the password for both authentication and privacy in the ***AuthPriv*** security level (step 208).

The following are exemplary entries that are generated in the SNMPv3 USM and VACM tables for initializing a DOCSIS cable modem in SNMPv3 mode. More specifically, the following exemplary entries (1-4a, b, c) are preferably pre-installed and initialized in the DOCSIS SNMPv3 compliant modem upon power-up:

(1) This entry (***usmUserEntry***) in the ***usmUserTable*** allows access to the system and ***tceDCM105Kickstart groups***. This entry allows the SNMP manager to read the modem's Diffie-Hellman public value (which is published by the agent in the ***tceDCMKickstartMyPublic*** MIB element) after registration has completed:

usmUserEngineID	localEngineID
usmUserName	"docsisInit"
usmUserSecurityName	"docsisInit"
usmUserCloneFrom	ZeroDotZero
usmUserAuthProtocol	none
usmUserAuthKeyChange	""
usmUserOwnAuthKeyChange	""
usmUserPrivProtocol	none
usmUserPrivKeyChange	""
usmUserOwnPrivKeyChange	""
usmUserPublic	""
usmUserStorageType	permanent
usmUserStatus	active

(2) An entry (***vacmSecurityToGroupEntry***) is generated in the ***vacmSecurityToGroupTable*** to map the initial user "docsisInit" into the accessible objects (i.e., this entry generates a ***groupName*** for the initial user "docsisInit," which is used to define an access control policy for the intial user):

vacmSecurityModel	3 (USM)
vacmSecurityName	"docsisInit"
vacmGroupName	"docsisInit"
vacmSecurityToGroupStorageType	permanent
vacmSecurityToGroupStatus	active.

(3) An entry (***vacmAccessEntry***) is generated in the ***vacmAccessTable*** translates the groupName for the intial user into appropriate view name (i.e., this entry defines the access rights for the intial user "docsisInit"):

vacmGroupName	"docsisInit"
vacmAccessContextPrefix	""
vacmAccessSecurityModel	3 (USM)
vacmAccessSecurityLevel	noAuthNoPriv
vacmAccessContextMatch	exact
vacmAccessReadViewName	"docsisInitRestricted"
vacmAccessWriteViewName	""
vacmAccessNotifyViewName	"docsisInitRestricted"
vacmAccessStorageType	permanent
vacmAccessStatus	active

The above entry in the ***vacmAccessTable*** is used for unauthenticated access, i.e., read-notify access for ***securityModel*** USM, ***securityLevel*** "noAuthNoPriv" on behalf of ***securityName*** (i.e., user "docsisInit") that belongs to the group "docsisInit" to the "docsisInitRestricted" MIB view in the default context with ***contextName*** "".

(4) The following three entries (***vacmViewTreeFamilyEntry***) are generated in the ***vacmViewTreeFamilyTable*** to allow the initial entry to access the system, kickstart groups, and generic traps:

(a)

vacmViewTreeFamilyViewName	"docsisInitRestricted"
vacmViewTreeFamilySubtree	1.3.6.1.2.1.1 (system)
vacmViewTreeFamilyMask	""
vacmViewTreeFamilyType	1 (included)
vacmViewTreeFamilyStorageType	permanent
vacmViewTreeFamilyStatus	active

(b)

vacmViewTreeFamilyViewName	"docsisInitRestricted"
vacmViewTreeFamilySubtree	(tceDCM105KickstartGroup)
vacmViewTreeFamilyMask	""

vacmViewTreeFamilyType	1 (included)
vacmViewTreeFamilyStorageType	permanent
vacmViewTreeFamilyStatus	active

(c)	*vacmViewTreeFamilyViewName*	"docsislnitRestricted"
	vacmViewTreeFamilySubtree	1.3.6.1.6.3.1.1.5 (snmpTraps)
	vacmViewTreeFamilyMask	""
	vacmViewTreeFamilyType	1
	vacmViewTreeFamilyStorageType	permanent
	vacmViewTreeFamilyStatus	active

The following entries (5-8a, b, c, d) are created in the SNMPv3 compliant modem when the Diffie-Hellman key exchange is completed.

(5) The following entry in the ***usmUserTable*** is associated with the provisioned user that is created with the authentication and privacy keys set by the DH key exchange. This entry is preferably created when the modem is correctly provisioned via entry of the manager's public value in the modem via the configuration file as explained above (step 202. 104 of Fig. 2). It is to be noted that the ***userName*** "docsisProv" gives at least full access to the ***usmUserTable*** for the created of additional valid user: and is preferably generated with the Authentication and privacy keys set by the DH Key exchange:

usmUserEngineID	localEngineID
usmUserName	"docsisProv"
usmUserSecurityName	"docsisProv"
usmUserCloneFrom	ZeroDotZero
usmUserAuthProtocol	usmHMACMD5AuthProtocol
usmUserAuthKeyChange	""
usmUserOwnAuthKeyChange	""
usmUserPrivProtocol	usmDESPrivProtocol
usmUserPrivKeyChange	""
usmUserOwnPrivKeyChange	""
usmUserPublic	""
usmUserStorageType	permanent
usmUserStatus	active

(6) The next entry maps the provisioned user "docsisProv" into the accessible objects:

vacmSecurityModel	3 (USM)
vacmSecurityName	"docsisProv"
vacmGroupName	"docsisProv"
vacmSecurityToGroupStorageType	permanent
vacmSecurityToGroupStatus	active

(7) The next entry translates the ***groupName*** for the provisioned user to a view name: user.

vacmGroupName	"docsisProv"
vacmAccessContextPrefix	""
vacmAccessSecurityModel	3 (USM)
vacmAccessSecurityLevel	AuthPriv
vacmAccessContextMatch	exact
vacmAccessReadViewName	"docsisProv"

vacmAccessWriteViewName	"docsisProv"
vacmAccessNotifyViewName	"docsisProv"
vacmAccessStorageType	permanent
vacmAccessStatus	active

(8) The following four entries allow the provisioned user read-write access to the system, *tceDCM105Kickstart*, usmMIBObjects, and vacmMIBObjects groups:

(a)

vacmViewTreeFamilyViewName	"docsisProv"
vacmViewTreeFamilySubtree	1.3.6.1.2.1.1 (system)
vacmViewTreeFamilyMask	""
vacmViewTreeFamilyType	1
vacmViewTreeFamilyStorageType	permanent
vacmViewTreeFamilyStatus	active

(b)

vacmViewTreeFamilyViewName	"docsisProv"
vacmViewTreeFamilySubtree	1.6.3.1.6.3.15.1(usmMIBObjects)
vacmViewTreeFamilyMask	""
vacmViewTreeFamilyType	1
vacmViewTreeFamilyStorageType	permanent
vacmViewTreeFamilyStatus	active

(c)

vacmViewTreeFamilyViewName	"docsisProv"
vacmViewTreeFamilySubtree	1.6.3.1.6.3.16.1(vacmMIBObjects)
vacmViewTreeFamilyMask	""
vacmViewTreeFamilyType	1
vacmViewTreeFamilyStorageType	permanent
vacmViewTreeFamilyStatus	active

(4)	*vacmViewTreeFamilyViewName*	"docsisProv"
	vacmViewTreeFamilySubtree	(tceDCM105KickstartGroup)\
	vacmViewTreeFamilyMask	""
	vacmViewTreeFamilyType	1
	vacmViewTreeFamilyStorageType	permanent
	vacmViewTreeFamilyStatus	active

In alternative embodiments of the present invention, other methods may be used to enter the manager's Diffie-Hellman public value into the modem and put it into SNMPv3 mode using proprietary configuration file elements (other than using an SNMP MIB object (configuration file element type 11) to set the ***tceDCM105KickstartMgrPublic*** MIB element as discussed above). These proprietary elements are particularly useful to initialize an SNMPv3 compliant modem in a SNMP network that has only SNMPv1/v2c modems which are not able to process a configuration file containing SNMP sets to the ***tceDCM105KickstartMgrPublic*** element and, consequently, cause the SNMPv1/v2c modems to reject the configuration file. For instance, the following configuration file elements may be used:

(1) ***tceKickStartMgrPublic*** *(element 180)* - This element comprises an octet string up to 128 bytes long with the manager's public value: and

(2) ***tceKickStartMgrPublic2*** (*element 181*)- This configuration file also comprises the managers public value. But in addition to putting the modem into SNMPv3 mode, it will cause the modem to translate the contents of a ***docsDevNmAccessTable*** (which is used for controlling access in SNMPv1/v2c) to corresponding entries in the SNMPv3 User, group, access, and view tables. More specifically, for each entry in the ***docsDevNmAccessTable***, a user and view is created with a ***userName*** set to the value in the community string and an access table entry that requires ***noAuthNoPriv*** security level. Also, entries are made in the SNMPv3 NOTIFICATION-MIB to cause traps to be sent to any trap receivers designated in the ***docsDevNmAccessTable.*** By using this configuration file element (181), the modem will be put in SNMPv3 mode and still be accessible by SNMPv2 managers. Details of this configuration file element and the associated translation process are described in the PCT patent application "*System and Method For Simple Network Management Protocol (SNMP)*

v3 Modems to Interoperate with SNMPv1/v2c Modems," Attorney Docket No RCA 89827 filed concurrently herewith.

In another embodiment, the public values P_1 and P_2 of the agent and manager may be exchanged using DHCP. For instance, the agent may include its public value in the DHCP request that is transmitted to the CMTS during the initialization process (as described above) and the manager's public value may be transmitted to the cable modem in the associated DHCP response. In particular, the following DHCP proprietary element ***tceDHCPKickstartMgrPublic*** (182) may be included in the DHCP response.

CLAIMS

1. A method for initializing a SNMP (simple network management protocol) v3 device, wherein an SNMP manager and an SNMP agent in the SNMPv3 device utilize a Diffie-Hellman key exchange protocol to enter an initial privacy key and an initial authentication key into the SNMPv3 device, wherein the SNMP manager and the SNMP agent both generate an associated random number and public value, wherein the SNMP manager passes its public value to the SNMP agent in a configuration file, wherein the SNMP manager reads the public value of the SNMP agent through a SNMP request using an initial valid user having access to the public value of the SNMP agent, and wherein the SNMP agent and SNMP manager compute a shared secret using the Diffie-Hellman key exchange protocol, wherein the method is characterized by the steps of:

converting the shared secret into a readable password;

converting the readable password into a secret key; and

setting an initial authentication key and an initial privacy key to the value of the secret key.

2. The method of claim 1, wherein the readable password comprises a 16 character password.

3. The method of claim 1, wherein the secret key comprises a 16 byte string.

4. The method of claim 1, further characterized in that the configuration file comprises a proprietary configuration file element for passing the public value of the SNMP manager to the SNMP agent.

5. The method of claim 4, wherein the SNMPv3 device operates in a SNMPv1/v2c enabled network comprising a SNMPv2c device, and wherein the proprietary configuration file element is ignored by the SNMPv2c device.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 April 2001 (05.04.2001)

PCT

(10) International Publication Number
WO 01/24444 A2

(51) International Patent Classification[7]: H04L 12/00

(21) International Application Number: PCT/US00/26060

(22) International Filing Date:
22 September 2000 (22.09.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/156,385 28 September 1999 (28.09.1999) US

(71) Applicant *(for all designated States except US)*: THOMSON LICENSING S.A. [FR/FR]; 46, quai Alphonse Le Gallo, F-92648 Boulogne Cedex (FR).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: YOST, William, Henry [US/US]; 101 West 103rd Street, Indianapolis, IN 46290 (US).

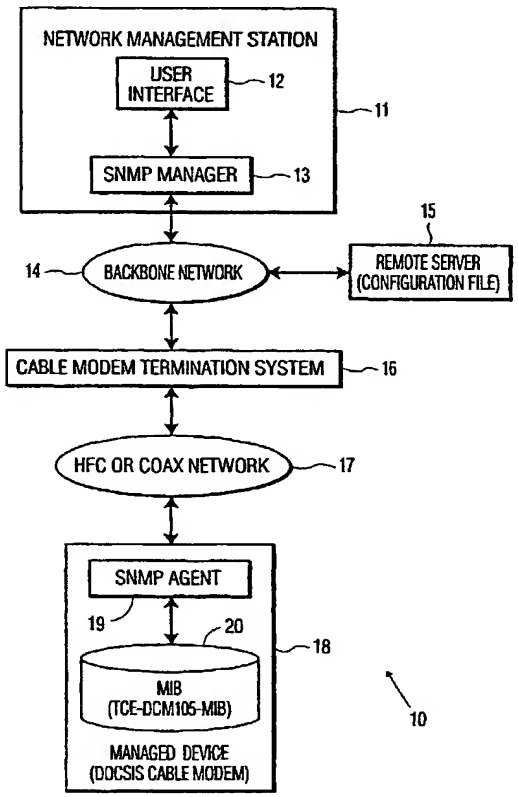
(74) Agents: TRIPOLI, Joseph, S. et al.; Thomson multimedia Licensing Inc., P.O. Box 5312, Princeton, NJ 08540 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR INITIALIZING A SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP) AGENT



(57) Abstract: A system and method for initializing an SNMP agent in SNMPv3 mode. In one aspect of the invention, a method is provided that allows an operator to securely enter the initial SNMPv3 privacy and authentication keys into an SNMPv3 device and cause the device to enter in SNMPv3 mode. The SNMP manager and SNMP agent both generate an associated random number and public value (steps 100, 101, 200, 201). The SNMP manager passes its public value to the SNMP agent in a configuration file, which causes a proprietary MIB element in the SNMPv3 device to be set with the public value of the SNMP manager (steps 202, 104). The SNMP manager reads the public value of the SNMP agent through an SNMP request using an initial valid user having access to the public value of the SNMP agent (steps 103, 203). The SNMP agent and SNMP manager each independently compute a shared secret using the Diffie-Hellman key exchange protocol (steps 105, 204). The SNMP manager and SNMP agent each independently convert the shared secret into the same readable password (steps 106, 205), convert the readable password into the same secret key (steps 107, 206) and set the initial authentication key and the initial privacy key to the value of the secret key (steps 108, 207).

WO 01/24444 A2

Published:

— *Without international search report and to be republished upon receipt of that report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

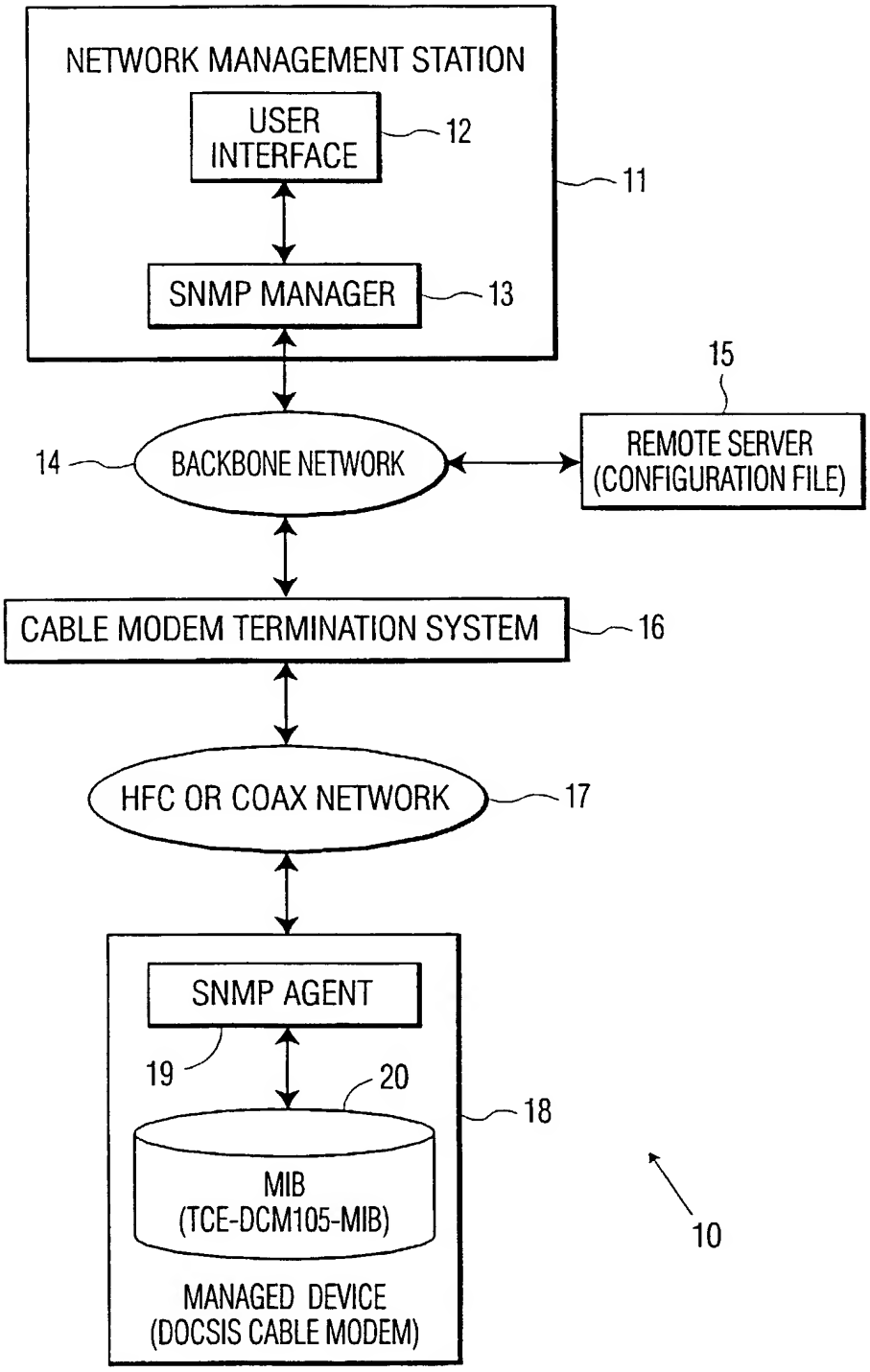

NETWORK MANAGEMENT STATION
USER INTERFACE
12
11
SNMP MANAGER
13
15
14
BACKBONE NETWORK
REMOTE SERVER (CONFIGURATION FILE)
CABLE MODEM TERMINATION SYSTEM
16
HFC OR COAX NETWORK
17
SNMP AGENT
19
20
18
MIB (TCE-DCM105-MIB)
MANAGED DEVICE (DOCSIS CABLE MODEM)
10

FIG. 1

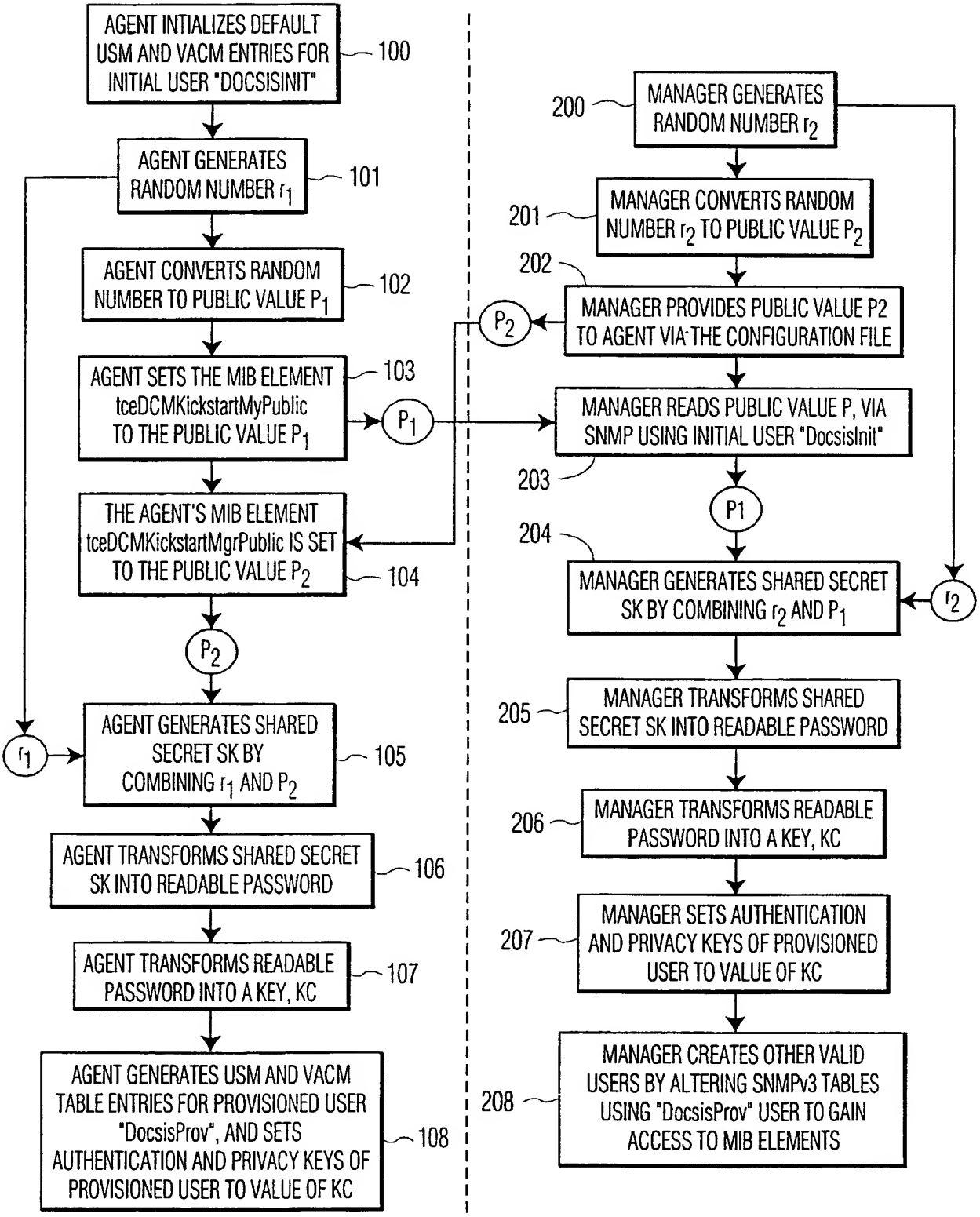

AGENT INTIALIZES DEFAULT USM AND VACM ENTRIES FOR INITIAL USER "DOCSISINIT"
100
AGENT GENERATES RANDOM NUMBER r_1
101
AGENT CONVERTS RANDOM NUMBER TO PUBLIC VALUE P_1
102
AGENT SETS THE MIB ELEMENT tceDCMKickstartMyPublic TO THE PUBLIC VALUE P_1
103
P_1
THE AGENT'S MIB ELEMENT tceDCMKickstartMgrPublic IS SET TO THE PUBLIC VALUE P_2
104
P_2
r_1
AGENT GENERATES SHARED SECRET SK BY COMBINING r_1 AND P_2
105
AGENT TRANSFORMS SHARED SECRET SK INTO READABLE PASSWORD
106
AGENT TRANSFORMS READABLE PASSWORD INTO A KEY, KC
107
AGENT GENERATES USM AND VACM TABLE ENTRIES FOR PROVISIONED USER "DocsisProv", AND SETS AUTHENTICATION AND PRIVACY KEYS OF PROVISIONED USER TO VALUE OF KC
108
200
MANAGER GENERATES RANDOM NUMBER r_2
201
MANAGER CONVERTS RANDOM NUMBER r_2 TO PUBLIC VALUE P_2
202
P_2
MANAGER PROVIDES PUBLIC VALUE P2 TO AGENT VIA THE CONFIGURATION FILE
MANAGER READS PUBLIC VALUE P, VIA SNMP USING INITIAL USER "DocsisInit"
203
P1
204
MANAGER GENERATES SHARED SECRET SK BY COMBINING r_2 AND P_1
r_2
205
MANAGER TRANSFORMS SHARED SECRET SK INTO READABLE PASSWORD
206
MANAGER TRANSFORMS READABLE PASSWORD INTO A KEY, KC
207
MANAGER SETS AUTHENTICATION AND PRIVACY KEYS OF PROVISIONED USER TO VALUE OF KC
208
MANAGER CREATES OTHER VALID USERS BY ALTERING SNMPv3 TABLES USING "DocsisProv" USER TO GAIN ACCESS TO MIB ELEMENTS

FIG. 2

Please type a plus sign (+) inside this box → [+]

PTO/SB/01 (10-00)
Approved for use through 10/31/2002. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

DECLARATION FOR UTILITY OR DESIGN PATENT APPLICATION (37 CFR 1.63)

☐ Declaration Submitted With Initial Filing **OR** ☒ Declaration Submitted after Initial Filing (surcharge (37 CFR 1.16 (e)) required)

Attorney Docket Number	RCA 89826
First Named Inventor	William Henry Yost
COMPLETE IF KNOWN	
Application Number	10/089,506
Filing Date	March 28, 2002
Group Art Unit	
Examiner Name	

As a below named Inventor, I hereby declare that:

My residence, post office address, and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

SYSTEM AND METHOD FOR INITIALIZING A SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP) AGENT

the specification of which *(Title of the Invention)*

☐ is attached hereto

OR

☒ was filed on (MM/DD/YYYY) 09/22/2000 as United States Application Number or PCT International Application Number PCT/US00/26060 and was amended on (MM/DD/YYYY) _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims as amended specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or 365(b) of any foreign application(s) for patent or inventor's certificate, or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or of any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY) Country	Priority Not Claimed	Certified Copy Attached? YES	NO
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐

☐ Additional foreign application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto:

I hereby claim the benefit under 35 U.S.C. 119(e) of any United States provisional application(s) listed below.

ApplicationNumber(s)	Filing Date (MM/DD/YYYY)	
60/156,385	09/28/1999	☐ Additional provisional application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

Please type a plus sign (+) inside this box → [+]

PTO/SB/01 (10-00)
Approved for use through 10/31/2002. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

DECLARATION — Utility or Design Patent Application

Direct all correspondence to: ☐ Customer Number or Bar Code Label [ ] OR ☐ Correspondance address below

Name	JOSEPH S. TRIPOLI
Address	THOMSON MULTIMEDIA LICENSING INC.
Address	PO Box 5312

City	State	ZIP
PRINCETON	NJ	08543-5312

Country	Telephone	Fax
USA	609-734-6807	(609) 734 - 6888

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

NAME OF SOLE OR FIRST INVENTOR: ☐ A petition has been filed for this unsigned inventor

1-00

Given Name	Family Name or Surname
WILLIAM HENRY	YOST

Inventor's Signature	Date
William Henry Yost	7/31/2002

Residence: City	State	Country	Citizenship
INDIANAPOLIS IN	IN	USA	USA

Mailing Address: 2346 Calaveras Way

Mailing Address

City	State	ZIP	Country
INDIANAPOLIS	IN	46240	USA

NAME OF SECOND INVENTOR: ☐ A petition has been filed for this unsigned inventor

Given Name	Family Name or Surname

Inventor's Signature		Date

Residence: City	State	Country	Citizenship

Mailing Address

Mailing Address

City	State	ZIP	Country

☐ Additional inventors are being named on the ____ supplemental Additional Inventor(s) sheet(s) PTO/SB/02A attached hereto.